(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－51951
（P2001－51951A）
(43)公開日　平成13年２月23日(2001.2.23)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｚ	５Ｂ０８５
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ	５Ｊ１０４
				９Ａ００１

審査請求　未請求　請求項の数５　ＯＬ　（全 8 頁）

(21)出願番号　特願平11－229542

(22)出願日　平成11年８月16日(1999.8.16)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　橋本　正一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　中原　慎一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100087848
弁理士　小笠原　吉義　（外１名）

最終頁に続く

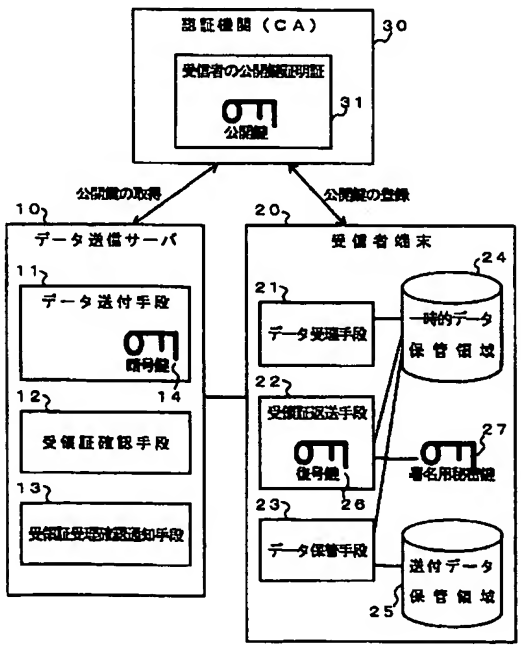
(54)【発明の名称】　電子データ配送システム，電子データ配送方法，電子データの受信者端末およびその受信者端末用プログラム記録媒体

(57)【要約】

【課題】　電子データ配送システムにおいて，ネットワークを介してデータを配送する際に，送信者が受信者から送付データの受理を証明する情報を受け取らない限り，受信者が受理した送付データの内容を確認できないようにする。

【解決手段】　データ送信サーバ10が，暗号鍵14を用いて暗号化した送付データを送ると，受信者端末20は，それを受理して一時的データ保管領域24に保管し，受領証返送手段22によって受信者に知られない方法により組み込まれた復号鍵26を用いて送付データを復号し，それに対して電子署名を生成し受領証として返送する。データ送信サーバ10は，受領証を確認すると，受領証受理確認通知を受信者端末20に送付する。受信者端末20は，受領証受理確認通知を受理後，暗号化された送付データを復号鍵26を用いて再度復号し，送付データ保管領域25に保管して，受信者がその内容を確認できるようにする。

本発明のシステム構成例



1

【特許請求の範囲】

【請求項１】　データ送信サーバと受信者端末とを有し，コンピュータネットワークを介して確かに電子データを送付したことの証拠情報を，データ送信サーバが受信者端末から受け取るための情報処理システムであって，前記データ送信サーバは，送付データを暗号鍵によって暗号化して，暗号化データを受信者端末へ送付するデータ送付手段と，前記受信者端末から受領証を受け取る受領証確認手段と，受領証を受理したことを受信者端末へ通知する受領証受理確認通知手段とを備え，前記受信者端末は，受理した暗号化データを一時的データ保管領域に一時的に保管するデータ受理手段と，受信者に知られない方法により組み込まれた復号鍵を用いて，受信者が内容を確認できない態様で前記受理した暗号化データを復号し，復号された送付データに対して，受領証となる電子署名を生成するための署名用秘密鍵を用いて受領証を作成し，前記データ送信サーバへ返送する受領証返送手段と，前記データ送信サーバから受領証受理確認通知を受け取った後に，前記暗号化データを復号鍵を用いて復号し，受信者が内容を確認できる態様で送付データ保管領域に復号した送付データを保管するデータ保管手段とを備えることを特徴とする電子データ配送システム。

【請求項２】　データ送信サーバと受信者端末とを有し，コンピュータネットワークを介して確かに電子データを送付したことの証拠情報を，データ送信サーバが受信者端末から受け取るための情報処理システムにおける電子データ配送方法であって，前記データ送信サーバは，送付データを該データ送信サーバ内に組み込まれた暗号鍵で暗号化して受信者端末へ送付し，前記受信者端末は，送付された暗号化データを一時的データ保管領域に保存し，該受信者端末内に組み込まれた復号鍵を用いて暗号化データを受信者に知られない方法で復号後，復号された送付データに対して署名用秘密鍵で電子署名を生成し，これを受領証として前記データ送信サーバへ返送し，前記データ送信サーバは，受理した受領証が送付データに対する受信者の電子署名であることを認証機関から取得した受信者の公開鍵証明証により確認して受領証を保存し，受領証を受理したことを示す受領証受理確認通知を前記受信者端末へ送付し，前記受信者端末は，前記データ送信サーバからの受領証受理確認通知を受理後，一時的データ保管領域に保管した暗号化データを再度復号鍵により復号し，復号された送付データを送付データ保管領域に保存することにより，データ送信サーバが，受信者端末から送付データを受理したことを証明する電子署名を受領証として受け取らない限り，受信者端末が受理した送付データの内容を確認することができないようにしたことを特徴とする電子データ配送方法。

【請求項３】　請求項２記載の電子データ配送方法において，前記受信者端末が受領証受理確認通知を受理できなかった場合に，前記受信者端末から再度前記データ送信サーバへ前記受領証を送り，前記データ送信サーバから受領証受理確認通知を再送してもらい，送付データの保管および内容の確認が可能になるようにしたことを特徴とする電子データ配送方法。

2

【請求項４】　コンピュータネットワークを介して，データ送信サーバから暗号化した電子データを受信する受信者端末であって，データ送信サーバから受信した暗号化データを一時的データ保管領域に一時的に保管するデータ受理手段と，受信者に知られない方法により組み込まれた復号鍵を用いて，受信者が内容を確認できない態様で前記受理した暗号化データを復号し，復号された送付データに対して，受領証となる電子署名を生成するための署名用秘密鍵を用いて受領証を作成し，前記データ送信サーバへ返送する受領証返送手段と，前記データ送信サーバから受領証受理確認通知を受け取った後に，前記暗号化データを復号鍵を用いて復号し，受信者が内容を確認できる態様で送付データ保管領域に復号した送付データを保管するデータ保管手段とを備えることを特徴とする電子データの受信者端末。

【請求項５】　コンピュータネットワークを介して確かに電子データを送付したことの証拠情報を，送信者が受信者から受け取るための電子データ配送システムにおける受信者端末を実現するためのプログラムを記録した記録媒体であって，データ送信サーバから受信した暗号化データを一時的データ保管領域に一時的に保管する処理と，受信者に知られない方法により組み込まれた復号鍵を用いて，受信者が内容を確認できない態様で前記受理した暗号化データを復号し，復号された送付データに対して，受領証となる電子署名を生成するための署名用秘密鍵を用いて受領証を作成し，前記データ送信サーバへ返送する処理と，前記データ送信サーバから受領証受理確認通知を受け取った後に，前記暗号化データを復号鍵を用いて復号し，受信者が内容を確認できる態様で送付データ保管領域に復号した送付データを保管する処理とを，計算機に実行させるプログラムを記録したことを特徴とする電子データの受信者端末用プログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，コンピュータネットワーク上でＥＤＩ（電子データ交換）やＥＣ（電子商取引）を実現するために必要となる電子データの配送システムにおいて，送信者が，受信者への電子データの送付と引き換えに，受信者から電子データを受理したことの証拠情報を受け取るためのシステムに関するものである。

【０００２】

【従来の技術】図６は，従来技術による電子データの送付に対する受領証の受け取り方法を示したものである。

【０００３】コンピュータネットワークを介して確かに電子データを送付したことの証拠情報を，送信者が受信者から受け取って保管しておきたい場合に，図６に示すように，送信者が送付対象データを作成して（Ｓ９１），受信者がこの送付した電子データを受理したら（Ｓ９２），受理した電子データに対する電子署名を生成してもらい（Ｓ９３），受信者にその生成した電子署名を受領の証として送付してもらって（Ｓ９４），送信者がこれを受け取る（Ｓ９５），という方法が考えられる。

【０００４】電子署名は，ＲＳＡやＥＳＩＧＮなどの公開鍵暗号を用いて実現される技術であり，電子データの保持者のみが所有する秘密鍵を用いて，署名対象の電子データを暗号化することにより生成されるため，署名者が署名対象の電子データを保持していたことの証拠情報となりうる。

【０００５】

【発明が解決しようとする課題】しかし，送信者が，電子データの送付と引き換えに，受信者からその電子データに対する電子署名を受領証として受け取りたい場合に，従来技術を用いると以下に示すような課題がある。

【０００６】受信者端末には，受信者が電子署名を生成する前に電子データが保存されるため，受信者が電子データの内容を確認後に意図的に受領証の返送を中止したり，受領証の返送中に通信路に障害が発生した場合には，受信者が電子データを受理しているにもかかわらず送信者が受領証を受け取ることができないという問題である。

【０００７】

【課題を解決するための手段】上記の課題を解決するため，本発明では，送信者が，受信者から送付データを受理したことを証明する電子署名を受領証として受け取らない限り，受信者が受理した送付データの内容を確認することができないことを特徴とした電子データ配送システムを提示する。以下において，本発明におけるシステム構成および本発明を実現するための手段について，図１，図２を用いて説明する。

【０００８】図１は，本発明のシステム構成例を示す図である。本発明のシステムは，データ送信サーバ１０，受信者端末２０，認証機関（ＣＡ）３０から構成される。

【０００９】〔データ送信サーバ〕データ送信サーバ１０は，組み込まれた暗号鍵１４を用いて送付データを暗号化し，これを受信者端末２０へ送付するためのデータ送付手段１１と，受信者端末２０からの受領証を受け取るための受領証確認手段１２と，受領証を受理したことを受信者端末２０へ通知するための受領証受理確認通知手段１３から構成される。

【００１０】〔受信者端末〕受信者端末２０は，データ送信サーバ１０から送付された暗号化データをディスク

上の一時的データ保管領域２４に保管するためのデータ受理手段２１と，受信者に知られない方法により組み込まれた復号鍵２６を用いて暗号化データを復号し，復号された送付データに対して受信者のみが知りうる署名用秘密鍵２７を用いて電子署名を生成し，この電子署名を受領証としてデータ送信サーバ１０へ返送するための受領証返送手段２２と，受信者が指定するディスク上の送付データ保管領域２５に送付データを保管するためのデータ保管手段２３から構成される。

【００１１】〔認証機関（ＣＡ）〕認証機関（ＣＡ）３０は，受信者が署名用秘密鍵２７と対で作成した署名用公開鍵を受信者から受け取り，それに対する公開鍵証明証３１を作成して保持する。

【００１２】図２は，本発明を実現する手段およびその処理の流れを示す図である。

ステップＳ１：データ送信サーバ１０のデータ送付手段１１は，本手段に組み込まれた暗号鍵１４を用いて送付データを暗号化し，その暗号化された電子データを受信者端末２０へ送付する。

【００１３】ステップＳ２：受信者端末２０のデータ受理手段２１は，ステップＳ１の処理で暗号化された送付データを受理し，これをディスク等の記憶装置上の一時的データ保管領域２４に保管する。

【００１４】ステップＳ３：受信者端末２０の受領証返送手段２２は，ステップＳ２の処理で保管した暗号化された送付データを本手段に組み込まれた復号鍵２６により復号し，復号された送付データに対して，受信者の署名用秘密鍵２７を用いて電子署名を生成する。そして，これを受領証としてデータ送信サーバ１０へ返送する。本手段は，電子署名を生成する過程において，復号された電子データの一部あるいは全ての情報に，受信者がアクセスできないように実現される。

【００１５】ステップＳ４：データ送信サーバ１０の受領証確認手段１２は，ステップＳ３の処理で送付された受領証を受理し，これが送付データに対する受信者の電子署名であることを，認証機関（ＣＡ）３０から取得した受信者の公開鍵証明証３１を用いて確認し，その受領証を保存する。

【００１６】ステップＳ５：データ送信サーバ１０の受領証受理確認通知手段１３は，ステップＳ４の処理の受領証の確認が終了した後，受領証を確かに受理したことを受信者端末２０へ通知する。

【００１７】ステップＳ６：受信者端末２０のデータ保管手段２３は，ステップＳ５の処理で送付された受領証受理確認通知を受理後，ステップＳ２の処理で一時的データ保管領域２４に保管した暗号化された送付データを，受領証返送手段２２に組み込まれた復号鍵２６を用いて復号し，復号された送付データを受信者が指定したディスク等の記憶装置上の送付データ保管領域２５に記録するとともに，一時的データ保管領域２４に保管され

ていた暗号化されたデータを削除する。また，通信路の障害等により受領証受理確認の通知が受理できなかった場合には，受領証がデータ送信サーバ１０に到達していない可能性があるため，上記ステップＳ３の処理以降を再度実行し，データ送信サーバ１０に受領証受理確認通知を送付してもらう。

【００１８】以上に示した手段による処理の流れにより，データ送信サーバ１０が受信者端末２０から受領証として送付データに対する受信者の電子署名を受理するまで，受信者端末２０において送付データの内容を受信者が確認できないようにすることが可能になる。

【００１９】以上の各処理手段を計算機によって実現するためのプログラムは，計算機が読み取り可能な可搬媒体メモリ，半導体メモリ，ハードディスクなどの適当な記録媒体に格納することができる。

【００２０】

【発明の実施の形態】本発明を実現するための具体的な実施の形態について，図３ないし図５を用いて説明する。図３は，本実施の形態におけるシステム構築時の処理の例を説明するための図，図４および図５は，本実施の形態におけるデータ送受信時の処理の例を説明するための図である。

【００２１】最初に，図３に従ってシステム構築時の処理について説明する。

（ａ１）暗号鍵・復号鍵の生成

受信者に知られない方法により，暗号鍵をデータ送信サーバ１０に，復号鍵を受信者端末２０に組み入れるため，信頼できる第三者または送信者の端末４０は，暗号鍵生成部４０１の機能を用いて暗号鍵１４と復号鍵２６を生成し，暗号鍵１４をデータ送付手段１１に，復号鍵２６を受領証返送手段２２とデータ保管手段２３に組み入れる。暗号鍵生成部４０１は，例えば既存の暗号ソフトウェア等により実現されている乱数発生機能を用いて実現可能である。

【００２２】（ａ２）暗号鍵・復号鍵のシステムへの組み込み

次に，信頼できる第三者または送信者の端末４０は，ファイル配送部４０２の機能を用いて，（ａ１）で生成したデータ送付手段１１をデータ送信サーバ１０へ配布し，受領証返送手段２２とデータ保管手段２３を受信者端末２０へ配布して，これらをそれぞれでインストールしてもらう。ファイル配送部４０２は，例えばＦＴＰなどを用いて実現可能である。なお，例えば信頼できる第三者または送信者の端末４０から，復号鍵を組み入れた受領証返送手段２２とデータ保管手段２３を個別に送るのではなく，データ受理手段２１，受領証返送手段２２およびデータ保管手段２３を実現するプログラムまたはスクリプトをまとめて，受信者端末２０へ送るようにしてもよい。

【００２３】また，信頼できる第三者または送信者の端末４０から，復号鍵を受領証返送手段２２およびデータ保管手段２３に組み入れて送る代わりに，復号鍵のみを暗号化などして受信者端末２０へ送り，あらかじめ受信者端末２０にインストールされた受領証返送手段２２およびデータ保管手段２３内に，受信者に認知できない方法で復号鍵を復号し組み入れる方法を用いてもよい。

【００２４】（ｃ１）受信者の署名用秘密鍵の生成

受信者端末２０は，署名用鍵対生成部２０１の機能を用いて署名用秘密鍵２７と公開鍵２８の鍵対を生成し，署名用秘密鍵２７は受信者端末２０に保存し，公開鍵２８は（ｃ２）の処理に用いる。署名用鍵対生成部２０１は，署名アルゴリズムに応じた秘密鍵２７と公開鍵２８のペアを生成する機能として，既存の暗号ソフトウェア等により実現されており，容易にこれを利用可能である。

【００２５】（ｃ２）受信者の署名用公開鍵の認証機関（ＣＡ）への登録

上記（ｃ１）で生成された鍵対のうち，データ送信サーバ１０が電子署名を検証する際に公開鍵２８を参照できるよう，公開鍵登録依頼部２０２の機能を用いて，公開鍵の認証機関である認証機関（ＣＡ）３０へ公開鍵２８を登録する。公開鍵登録依頼部２０２は，例えば認証機関（ＣＡ）３０が提供する公開鍵登録サービスを利用することにより実現可能である。

【００２６】（ｄ１）公開鍵証明証の作成

認証機関（ＣＡ）３０は，（ｃ２）で依頼された公開鍵２８に対して，公開鍵証明証発行部３０１の機能を用いて受信者の公開鍵証明証３１を作成し，これを認証機関（ＣＡ）３０内に保管する。公開鍵証明証発行部３０１の機能は，公開鍵に対してその所有者や有効期限など証明する公開鍵証明証を作成する機能であり，既存の認証機関（ＣＡ）システムにおいて実現されている機能である。

【００２７】データ送信サーバ１０と受信者端末２０との間でデータ送受信は，例えば図４および図５に示すように行われる。

【００２８】〔１〕受信者端末２０へのデータの送付（データ送信サーバ１０）

データ送信サーバ１０のデータ送付手段１１は，ファイルアクセス部１１１の機能を用いて，受信者へ送付するデータを読み出し（Ｓ１１），データ暗号化部１１２の機能を用いて，データ送付手段１１に組み込まれている暗号鍵１４により送付データを暗号化する（Ｓ１２）。そして，データ通信部１１３の機能を用いて，暗号化された送付データ７１を受信者端末２０へ送付する（Ｓ１３）。ファイルアクセス部１１１は，コンピュータシステムで一般に提供されている機能であり，容易に利用可能である。また，データ暗号化部１１２は，暗号鍵１４と暗号化したいデータを入力として暗号化データを出力する機能であり，既存のＦＥＡＬやＤＥＳなどの暗号技

術を用いて容易に実現可能である。データ通信部１１３は，例えばＴＣＰ／ＩＰ通信などが利用可能であり，一般のコンピュータシステムにおいて実現されている機能である。

【００２９】〔２〕暗号化された送付データの受理（受信者端末２０）

受信者端末２０のデータ受理手段２１は，データ通信部２１１の機能を用いてデータ送信サーバ１０からの暗号化された送付データ７１を受信し（Ｓ２１），ファイルアクセス部２１２の機能を用いてこれをディスク等の記憶装置上の一時的データ保管領域２４へ記録する（Ｓ２２）。

【００３０】〔３〕受領証の作成・返送（受信者端末２０）

受信者端末２０の受領証返送手段２２は，ファイルアクセス部２２１の機能を用いて，上記〔２〕の処理で保管した暗号化データを読み出し（Ｓ３１），データ復号化部２２２の機能を用いて，受信者端末２０に組み込まれている復号鍵２６により暗号化データをメモリ上に復号する（Ｓ３２）。続いて，メモリ上に復号された送付データに対して，ハッシュ化部２２３の機能を用いてハッシュ値を生成し，このハッシュ値に対して署名生成部２２４の機能を用いて，受信者の署名用秘密鍵２７により電子署名を生成し，これを受領証７２とする（Ｓ３３）。そして，最後にデータ通信部２２５の機能を用いて，この受領証７２をデータ送信サーバ１０へ返送する（Ｓ３４）。データ復号化部２２２は，暗号化データと復号鍵を入力として復号結果を出力する機能であり，データ暗号化部１１２と対になる機能として既存の暗号技術を用いて容易に実現可能である。ハッシュ化部２２３として，例えばＳＨＡ－１やＭＤ５などのアルゴリズムが，ハッシュ値を暗号化し署名を生成する署名生成部２２４として，例えばＥＳＩＧＮやＲＳＡなどのアルゴリズムが広く知られており，どちらも既存の暗号ソフトウェア等により実現されており，容易に利用可能である。

【００３１】また，本手段における電子署名を生成する過程（Ｓ３１～Ｓ３３）の各処理において，復号された送付データ７１の情報は，ディスク等の記憶装置上に書き込まれないため，端末の障害等の発生により処理が中断して電子署名が生成されなかった場合でもその情報が残らず，受信者が送付データ７１の内容を確認することはできない。

【００３２】〔４〕受領証の確認（データ送信サーバ１０）

データ送信サーバ１０の受領証確認手段１２は，まず，データ通信部１２１の機能を用いて，上記〔３〕の処理で送付された受領証７２を受理する（Ｓ４１）。次に，受理した受領証７２が，送付データ７１に対して受信者が生成した電子署名であることを検証するため，電子署名の検証に必要な受信者の公開鍵証明証３１を，公開鍵取得部１２２の機能を用いて認証機関（ＣＡ）３０から取得し（Ｓ４２），送付データ７１をファイルアクセス部１２３の機能を用いて再度取得した後（Ｓ４３），署名検証部１２４の機能を用いて電子署名の検証を行い，その正当性を判定する（Ｓ４４）。そしてこの検証の後，受領証７２をファイルアクセス部１２５の機能を用いて保存する（Ｓ４５）。

【００３３】公開鍵取得部１２２は，受信者の公開鍵を認証機関（ＣＡ）３０から取得する機能であり，例えばディレクトリ参照機能を用いて実現可能である。署名検証部１２４は，電子署名，署名者の公開鍵２８，署名対象データを入力として，電子署名が署名対象データに対して署名者の署名用秘密鍵２７により生成されたことを確認する機能であり，署名生成部２２４と対となる機能として既存の暗号ソフトウェア等により実現されており，容易に利用可能である。

【００３４】〔５〕受領証受理の確認通知（データ送信サーバ１０）

データ送信サーバ１０の受領証受理確認通知手段１３は，上記〔４〕の処理の受領証の確認が正常に終了した後，ファイル編集部１３１の機能を用いて受領証を受理したことを受信者端末２０へ通知するための受領証受理確認通知７３を作成し（Ｓ５１），これをデータ通信部１３２の機能を用いて受信者端末２０へ送付する（Ｓ５２）。ファイル編集部１３１は，例えばエディタ機能を用いるなど，通常のコンピュータシステムが提供する機能を用いることで実現でき，容易に利用可能である。

【００３５】〔６〕データの保管（受信者端末２０）

受信者端末２０のデータ保管手段２３は，データ通信部２３１の機能を用いて，上記〔５〕の処理で送付された受領証受理確認通知７３を受理した後（Ｓ６１），ファイルアクセス部２３２の機能を用いて，上記〔２〕の処理で一時的データ保管領域２４に保管した暗号化データを読み出し（Ｓ６２），データ復号化部２３３の機能を用いて，受信者端末２０に組み込まれた復号鍵２６により暗号化データを復号し（Ｓ６３），ファイルアクセス部２３４の機能を用いて，復号化された送付データ７１を受信者が指定したディスク等の記憶装置上の送付データ保管領域２５に保管するとともに，保管されていた暗号化データを削除する。また，一定時間経っても受領証受理確認通知７３が受理できない場合には，一時的データ保管領域２４に保管されている暗号化データに対して，〔３〕以降の処理を再度繰り返す。

【００３６】以上に示した処理を実現することにより，受信者端末２０のディスク等の記憶装置上には，データ送信サーバ１０が受信者端末２０から受領証として送付データ７１に対する受信者の電子署名を受理するまで，復号された送付データ７１が書き込まれないため，受信者が受領証を返送せずに送付データの内容を確認することの防止が可能になる。

【００３７】

【発明の効果】以上の説明から明らかであるように，本発明によれば，受信者が受理した電子データの内容を確認する前に，必ず受理した電子データに対する受領証を送信者が受信者から受け取ることができるため，送信者は受信者に対して情報の提供と引き換えにこの受領証を元にして，後日，課金の請求等を行うことが可能になる。また，受信者は受領証を送付するまで送付されたデータの内容を確認することができないため，送付されたデータの内容によって受領証を返すか返さないかの判断を受信者が行うことを不可能にすることができる。

【図面の簡単な説明】

【図１】本発明のシステム構成例を示す図である。

【図２】本発明を実現する手段およびその処理の流れを示す図である。

【図３】本実施の形態におけるシステム構築時の処理を説明するための図である。

【図４】本実施の形態におけるデータ送受信時の処理（データ送信サーバ側）を説明するための図である。

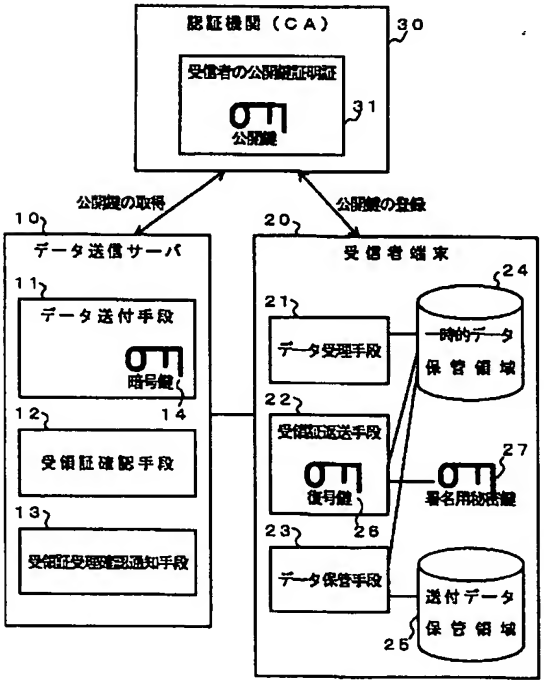
【図５】本実施の形態におけるデータ送受信時の処理（受信者端末側）を説明するための図である。

【図６】従来技術による電子データ送付方法を示す図である。

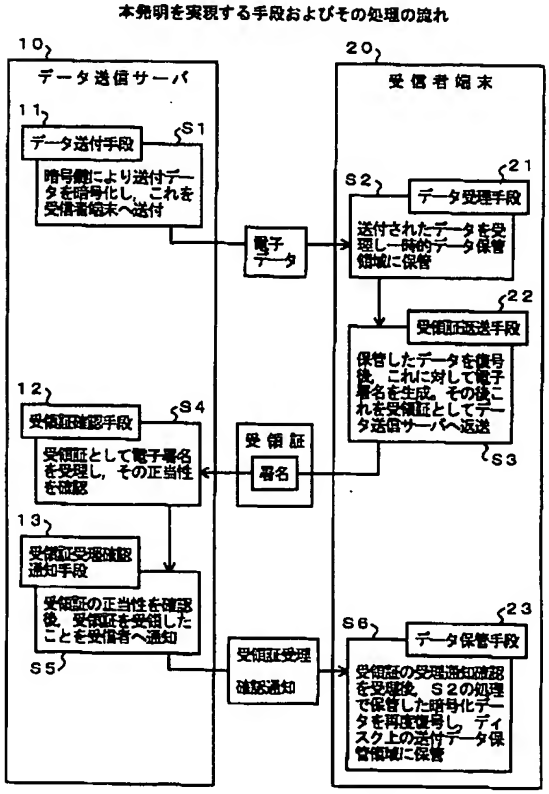
【符号の説明】

１０　データ送信サーバ
１１　データ送付手段
１２　受領証確認手段
１３　受領証受理確認通知手段
１４　暗号鍵
２０　受信者端末
２１　データ受理手段
２２　受領証返送手段
２３　データ保管手段
２４　一時的データ保管領域
２５　送付データ保管領域
２６　復号鍵
２７　署名用秘密鍵
３０　認証機関（ＣＡ）
３１　受信者の公開鍵証明証

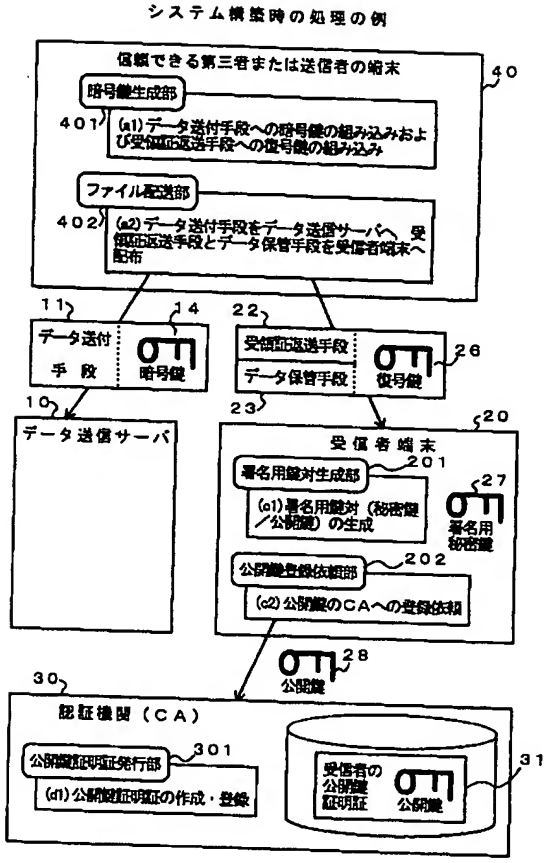
【図１】



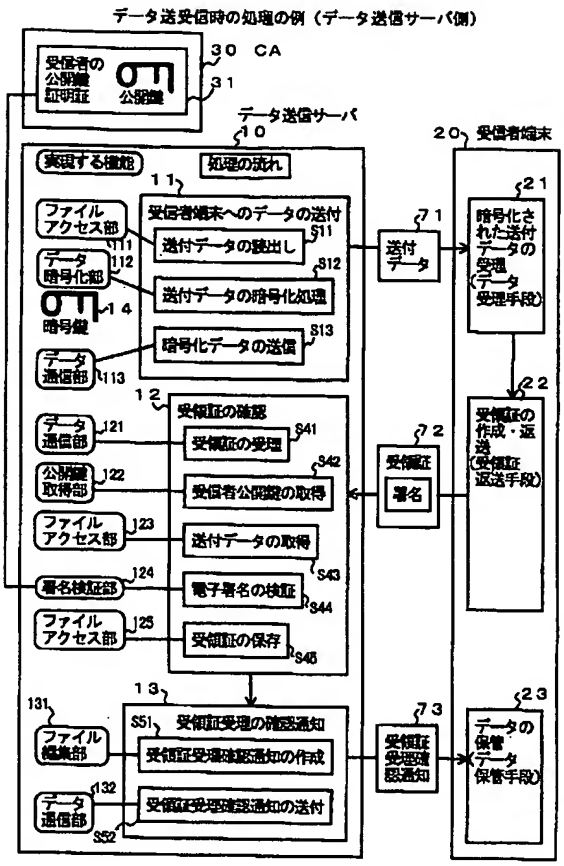
【図２】



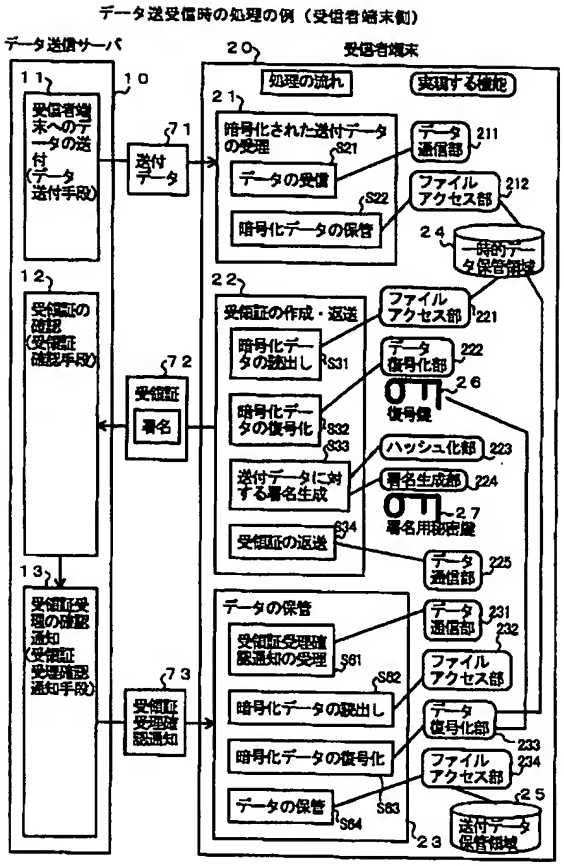
【図３】


システム構築時の処理の例
信頼できる第三者または送信者の端末
40
暗号鍵生成部
401
(a1)データ送付手段への暗号鍵の組み込みおよび受領証返送手段への復号鍵の組み込み
ファイル配送部
402
(a2)データ送付手段をデータ送信サーバへ、受領証返送手段とデータ保管手段を受信者端末へ配布
11
データ送付手段
14
暗号鍵
22
受領証返送手段
データ保管手段
26
復号鍵
23
10
データ送信サーバ
受信者端末
20
署名用鍵対生成部
201
(a1)署名用鍵対（秘密鍵／公開鍵）の生成
27
署名用秘密鍵
公開鍵登録依頼部
202
(a2)公開鍵のCAへの登録依頼
28
公開鍵
30
認証機関（CA）
公開鍵証明証発行部
301
(d1)公開鍵証明証の作成・登録
受信者の公開鍵証明証
公開鍵
31

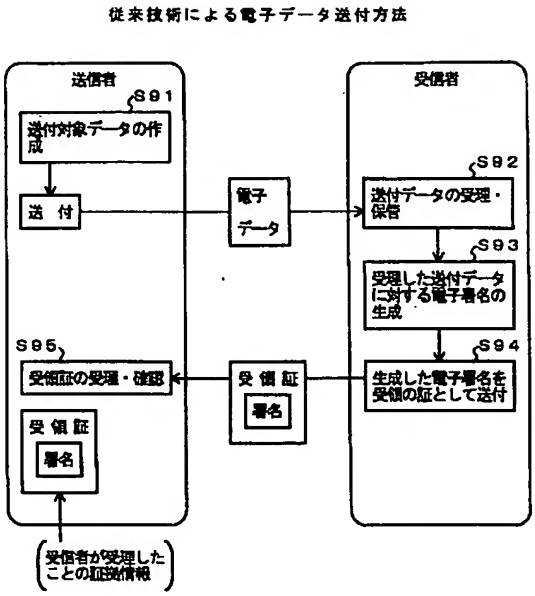
【図４】


データ送受信時の処理の例（データ送信サーバ側）
受信者の公開鍵証明証
公開鍵
30 CA
31
データ送信サーバ
10
20 受信者端末
実現する機能
処理の流れ
11
ファイルアクセス部
111
受信者端末へのデータの送付
送付データの読出し
S11
データ暗号化部
112
S12
送付データの暗号化処理
暗号鍵
14
S13
暗号化データの送信
データ通信部
113
12
受領証の確認
データ通信部
121
受領証の受理
S41
公開鍵取得部
122
受信者公開鍵の取得
S42
ファイルアクセス部
123
送付データの取得
S43
署名検証部
124
電子署名の検証
S44
ファイルアクセス部
125
受領証の保存
S45
13
131
ファイル編集部
S51
受領証受理確認通知の作成
データ通信部
132
受領証受理確認通知の送付
S52
71
送付データ
72
受領証
署名
73
受領証受理確認通知
21
暗号化された送付データの受理（データ受理手段）
22
受領証の作成・返送（受領証返送手段）
23
データの保管（データ保管手段）

【図５】



【図６】



フロントページの続き

Ｆターム(参考)　5B085 AE06 AE13 AE29 CA04
5J104 AA01 AA09 EA16 JA21 LA06
NA02 PA07 PA10
9A001 EE03 JJ65 JJ67 LZ03